has a latent mental condition or the defendant caused all of the harm, then the defendant is liable for all of the mental harm sustained by the plaintiff.[60] If, however, PTSD is classified as a preexisting mental condition, then courts have held the defendant to be liable only for aggravation of the condition.[61]

Case Law

Traditionally, the "thin skull" plaintiff rule was applied by the majority of jurisdictions to physical injuries. With the wider acceptance of mental injuries came a broader application of the "thin skull" plaintiff rule. In the 1998 case *Poole v. Copland, Inc.*, the North Carolina Supreme Court affirmed a decision by the North Carolina Court of Appeals that enabled the "thin skull" rule to apply to mental injury cases.[62] Here, a former employee sued her former co-worker alleging both intentional and negligent infliction of emotional distress.[63] Under the doctrine of respondeat superior, she also sued the employer.[64] The employee ultimately prevailed, recovering actual and punitive damages "resulting from a flashback of repressed memories of childhood sexual abuse

---

[60] *Salas v. United States*, 974 F. Supp. 202, 209 (W.D.N.Y. 1997) (relaying that the defendant "may be liable for damages for aggravation of a pre-existing illness or for precipitation of a latent condition"); *Calcagno v. Kuebel, Fuchs P'ship*, 01-691 (La. App. 5 Cir. Nov. 14, 2001), 802 So. 2d 746, 752 (holding the defendant completely accountable for all of the mental harm because the physical injury activated age-related changes in the brain that were previously asymptomatic); *LaSalle v. Benson Car Co.*, 00-1459 (La. App. 5 Cir. Jan. 30, 2001), 783 So. 2d 404, 408-09 (holding that all of the plaintiff's mental harm was caused by the defendant because prior to the physical injury, the plaintiff had no psychological problems, but subsequently required psychiatric treatment).

[61] See *Salas*, 974 F. Supp. At 209; *Touchard v. Slemco Electric Foundation*, 99-3577, P 1 (La. Oct. 17, 2000), 769 So. 2d 1200, 1202 (expressing that because the plaintiff's injuries were preexisting, it was up to the jury to decide whether the defendant aggravated them).

[62] *Poole v. Copland*, 348 125 N.C. App. 235, 481 S.E.2d 88 (1997), aff'd, 348 N.C. 260, 498 S.E.2d 602 (1998).

[63] *Id.* at 236, 481 S.E.2d at 89.

[64] *Supra* note 78.

when aggravated by the on-the-job sexual harassment."[65] Significantly, her susceptibility to triggers causing severe emotional distress were recognized and she recovered the full extent of her damages.[66] And, for the first time, the North Carolina Supreme Court afforded the application of the "thin skull" plaintiff rule to mental injury cases.[67]

In New York, a district court grappling with determining liability when mental harm accompanies physical injuries illustrates a conundrum many courts face.[68] In *Salas v. United States*, a forty-nine year old teacher was involved in a 1991 car accident when the defendant ran a stop sign.[69] At the emergency room, she was diagnosed with minor injuries, yet she continued to experience severe symptoms disproportionate to the physical injuries.[70] Five years later, at the time of trial, the plaintiff continued to suffer from "extreme anxiety, confusion, pain in virtually every part of her body, and limited affect."[71] Medical experts agreed that she was not "malingering,"[72] rather she was suffering disproportionately to the severity of the accident, thereby implicating a psychological component.[73] Rejecting the defendant's notion that the plaintiff had a preexisting medical condition that would have caused her harm independent of the

---

[65] *Id.* at 180, citing Poole, 348 N.C. at 264, 498 S.E.2d at 604.
[66] *Id.*
[67] North Carolina had taken steps toward this result in two earlier cases. In *Potts v. Howser*, 274 N.C. 49, 52, 161 S.E.2d 737, 742 (1968), the North Carolina Supreme Court indicated that the "think skull" plaintiff rule included aggravating or activating a pre-existing physical or mental condition. Even before that, in *Johnson v. Ruark Obstetrics*, 395 S.E.2d 85, 90 (1890), the North Carolina Supreme Court relayed that "mental injury is simply another type of 'injury'—like 'physical' or 'pecuniary' injuries."
[68] *Salas*, 974 F. Supp. at 209.
[69] *Id.* at 204.
[70] *Id.*
[71] Robert Jean Campbell, Campbell's Psychiatric Dictionary 15 (Oxford University Press 2004) (1940) (defining affect as "a person's disposition to react emotionally in certain specific ways…the fluctuating, subjective aspect of emotion.").
[72] *Id.* at 383 (defining malingering as the intentional exaggeration of physical symptoms).
[73] *Salas*, 974 F. Supp. at 205.

accident, the court never expressly indicated whether the plaintiff had a previous mental condition or had a latent mental condition.[74] Unfortunately, the court never explained how its decision was reached, nor did it provide elements of a test for future courts to apply.[75]

The problem is not with courts recognizing liability for mental harm; instead, it is how the "thin skull" plaintiff rule is applied to mental harm accompanying physical injury.[76] Courts have not reached a consensus on differentiating between a latent and preexisting mental condition. A dormant "disorder that has not erupted into full-blown psychotic symptoms" qualifies as a latent mental condition.[77] A latent mental condition can be analogized to the Newtonian physics notion that "an object at rest remains at rest unless acted on by an outside force." Likewise, a latent mental condition exists but the outside event causes it to "move."[78]

In contrast, "a preexisting mental condition is a condition that existed before the physical injury occurred, was symptomatic, and affected the plaintiff's functioning in daily life."[79]

Where does PTSD fall along this continuum? PTSD encompasses both a physical and a mental injury and requires an outside actor or event to trigger the condition.

---

[74] *Id.* at 208-13.
[75] *Id.*
[76] J. Stanley McQuade, *The Eggshell Skull Rule and Related Problems in Recovery for Mental Harm in the Law of Torts*, 24 Campbell L. Rev. 1, 2-3 (2001).
[77] *Supra* note 93 at 366.
[78] *Walton v. William WolfBaking Co.*, 406 So. 2d 168, 171-73 (La. 1981) (illustrating that the court held that the plaintiff either had no mental condition before the accident or had a latent mental condition, but rejected defendant's arguments that the plaintiff had a preexisting mental condition).
[79] Renka, 29 T. Jefferson L. Rev. at 293, *citing*

Therefore, unlike a case such as *Salas*,[80] where the plaintiff received different mental disorder diagnoses ranging from schizo-affective disorder to borderline personality from various experts, individuals diagnosed with PTSD have much clearer parameters. PTSD is the only mental medical condition that *requires* an outside event or actor in order to cause physical brain damage and trigger mental symptoms.[81] Therefore, because of the unique nature of PTSD having mental and physical harm components, the "thin skull" plaintiff rule should render the defendant liable for all of the plaintiff's mental and physical harm, and not merely liable for aggravation of a mental condition.

In relation to the "thin skull" plaintiff rule, the defendant is liable for aggravation of an already present condition, whether classified as preexisting or latent, regardless of whether the aggravation was foreseeable.[82] The difference in terming the condition preexisting or latent is the impact on the damages. Often times a defendant will skew the preexisting condition to argue that the condition, and not the defendant's tortious acts, is a partial or substantial cause of the injuries.[83] Even when defendants have attempted to use this type of evidence in this manner, courts have held to the contrary.[84]

---

[80] *Salas*, 974 F. Supp. at 206-07 (holding that the plaintiff's "emotional problems were caused by the accident" because every expert testified that she was able to cope before but not after the accident. Although there was conflicting testimony of whether the condition was preexisting or latent, the court found that a lone dissenting expert will not defeat causation).

[81] *Supra* note 55.

[82] Restatement (Third) of Torts: Liability for Physical Harm §26 cmt. K (Proposed Final Draft No. 1, 2005).

[83] *Supra* note 106 at 762.

[84] *Freeman v. Busch*, 349 F.3d 582, 590 (8th Cir. 2003) (entitling the plaintiff in a civil sexual assault case to the "thin skull" instruction based upon evidence that she had received prior treatment for sexual abuse and that the condition was exacerbated by the alleged rape); *Hare v. H&R Indus.*, No. 00-CV-4533, 2002 WL 777956, at 2 (E.D. Pa. Apr. 29, 2002) (holding that despite other factors contributing to the plaintiff's psychiatric hospitalization subsequent to the sexual harassment incident, the defendant was still liable for all of the medical expenses on the premise of the "thin skull" plaintiff rule plus the difficulty in apportioning the harms).

PTSD is dependent upon an external stimulus, just like stress or exertion aggravates angina (an area of the heart deprived of oxygen-rich blood causing pain)[85], so there is less ambiguity in terms of causation. The ordinary minds for whom our rules of evidence were created, should be able to recognize that PTSD is the only psychiatric condition requiring an outside actor/event to trigger the condition that produces both a physical and mental injury. Still, it is incumbent upon courts to scrutinize what evidence is admissible so that the probative value is not outweighed by a prejudicial impact.

PTSD: Mental or Physical Injury for the Purposes of the "Thin Skull" Application

PTSD is both a mental and a physical injury. That is, PTSD qualifies as a mental injury per DSM-IV.[86] But, due to evidence that the hippocampus, frontal premedial cortex, and neurons experience physical damage when the initial trauma or recurring triggering event occurs, PTSD should also be plead as a physical injury.[87] Hence, in the case of PTSD, the argument that "a mental injury may be completely subjective in its diagnosis, origin, and treatment"[88] is invalid.

Diagnostic testing, such as an MRI of the brain, has not been sanctioned by the American College of Radiologists as a stand alone means of determining a post-traumatic condition.[89] While post-traumatic conditions have been included as an extended

---

[85] National Institute of Health, *What Is Angina?*, *available at* www.nhlbi.nih.gov/health/dci/Diseases/Angina/Angina_WhatIs.html.
[86] *Supra* note 19.
[87] Bremner, *supra* note 6; Kennedy, *supra* note 40.
[88] *Supra* note 78.
[89] American College of Radiologists, *Practice Guideline for the Performance and Interpretation of Magnetic Resonance Imaging (MRI) of the Brain*, Revised 2008, *available at* www.acr.org/SecondaryMainMenuCategories/.../guidelines/.../mri_brain.aspx. "These guidelines are an educational tool designed to assist practitioners in providing appropriate radiologic care for

indication of an MRI, the totality of the circumstances and other diagnostic criteria need to be considered.[90] Because "the practice of medicine involves not only the science, but also the art of dealing with the prevention, diagnosis, alleviation, and treatment of disease," solely relying on a radiographic image for post-traumatic conditions is not determinative of the existence of PTSD.[91] Like endometriosis, an enigmatic condition, just because a condition may not appear on diagnostic radiographs and images does not mean that it does not exist.[92] Because of the increasing amount of documentation available, it is clear that post-traumatic stress disorder includes both a mental and physical harm component. Hence, it is unreasonable to contend that the diagnosis of PTSD is completely subjective.

The Relevance BCE's Reckless Acts and Ms. Roe's Past Experiences

In a December 15, 2011 email, Mr. Davidson suggested, "[m]ore going on than a legitimate claim by Ms. Roe. To that end, I am trying to balance the need to protect BCE with a genuine concern about her state of mind and her well-being, and certainly do not want to create bigger issues not just for her, but for BCE as well." (Ex.). In light of the escalating tension and retaliation from BCE, on September 13,

---

patients. They are not inflexible rules or requirements of practice and are not intended, nor should they be used, to establish a legal standard of care. For these reasons and those set forth below, the American College of Radiology cautions against the use of these guidelines in litigation in which the clinical decisions of a practitioner are called into question. The ultimate judgment regarding the propriety of any specific procedure or course of action must be made by the physician or medical physicist in light of all the circumstances presented. Thus, an approach that differs from the guidelines, standing alone, does not necessarily imply that the approach was below the standard of care."

[90] *Id.*

[91] *Id.* at p. 1.

[92] Jane V. Roe, *Cutting Funds for Oral Contraceptives: Violation of Equal Protection Rights and the Disparate Impact on Women's Healthcare*, The Modern American, Spring 2009, p. 23; Cleveland Clinic, *Facts About Endometriosis*, *available at* www.my.clevelandclinic.org/disorders/endometriosis/hic_facts_about_endometriosis.aspx.

2011, following a clinical discussion in Midland, TX with Dr. Weinman on the subject of PTSD, Ms. Roe forwarded an article she co-authored entitled, *Another Crack in the Thin Skull Plaintiff Rule: Why Women with Post Traumatic Stress Disorder Who Suffer Physical Harm from Abusive Environments at Work or School Should Recover from Employers and Educators.* (Ex.) The article addresses workplace harassment, the medical impact and the liability for employers.

Regarding Ms. Roe's "state of *mind,*" after discussing the abusive situations that occurred at BCE over a period of time with a dual-board certified physician qualified to make a determination, Ms. Roe's state of mind is not an issue. This is further supported by her communications and presentation reviews from various organizations that occurred before and after she tendered her resignation on December 5, 2011. (Ex.)

In light of Dr. Weinman knowing of at least one instance of sexual trauma that affected her and still hugging her with his hands in the small of her back and kissing her on the lips on various separate occasions including: January 23, 2011 (Birmingham, AL); January 25, 2011 (Birmingham, AL); and March 30, 2011 (Midland, TX). And , even with the knowledge of her experiencing a trauma, which she relayed after Dr. Weinman told her on April 14, 2011 in Atlanta, GA of his wife's traumatic sexual history, which included being sexually assaulted by a treating mental health care provider, his actions did not change. Moreover, acknowledging Mr. Bill Gross's referring to her as "little girl", having discussed and received a legal scholarly article co-authored by Ms. Roe on the affects of PTSD and being a physician, BCE recklessly initiated the triggering events, which included inappropriate comments and kissing her

on the lips on four instances that, in turn, caused harm to Ms. Roe.

THE STORED COMMUNICATIONS ACT AND DEFENDANTS' CONDUCT

This portion is derived in part from a forthcoming ABA article.[93]

In an era of electronic communication services and remote computing services being utilized to transmit protected health information (PHI), it is necessary to consider the Stored Communications Act.[94] As part of the Act, Congress sought to regulate: (1) electronic communication services (ECS), and (2) remote computing services (RCS).[95] ECS encompasses "data transmission and electronic mail," while RCS includes outsourced computer processing and data storage.[96] An increasingly utilized type of RCS is cloud computing. "Cloud Computing Services are an emerging network architecture by which data and applications reside on third party servers, managed by private firms, which provide remote access through web-based devices."[97] In essence, users can share or store their own information on remote servers owned by others and gain access via the

---

[93] Rachel V. Rose, *Above the Clouds: Not Guarding Protected Health Information in the Era of Electronic Communications and Remote Computing May Lead to a Viable Action Under the False Claims Act* (publication forthcoming, the American Bar Association, 2012).

[94] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 201, 100 Stat. 1848, 1860-68 (codified as amended at 18 U.S.C. §§ 2701-2711); *see also*, William Jeremy Robison, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 The Georgetown Law Journal 1195, 1196 (2010), *citing* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1208 n. 1 (2004) (noting the common reference to Title II of the Electronic Communications Privacy Act as the "Stored Communications Act").

[95] H.R. Rep. No. 99-647, at 21, 23.

[96] *Id.*

[97] FTC Complaint of Electronic Privacy Information Center at 4, *In re* Google, Inc. & Cloud Computing Servs. (Mar. 19, 2009).

Internet or through other connections.[98]

Enacted in 1986, the Stored Communications Act (SCA) is the primary federal source of electronic privacy protections.[99] It was enacted a decade before HIPAA and over two decades prior to the HITECH Act. Yet, it is important for several reasons. First, it is the foundation for privacy in relation to electronic communications and storage. Second, courts have been the primary source for interpretation of related privacy issues. Finally, SCA judicial precedents provide valuable insight into how service agreements and privacy policies are interpreted in relation to privacy. A court's propensity to uphold the legislative intent of the SCA and the U.S. Supreme Court's Fourth Amendment case holdings reinforce Congress' policy purpose behind HIPAA. Therefore, providers of electronic transmissions and storage, who are considered either a business associate or a subcontractor under the HITECH Act, should also read the SCA, relevant case law and U.S. Supreme Court Fourth Amendment landmark privacy cases *Katz v. United States*, 389 U.S. 347 (1967) and *Smith v. Maryland*, 442 U.S. 735 (1979), and *United States v. Jones*, 565 U.S. (2012)[100] *in pari materi* to fully appreciate the extent of liability in relation to their contracts.

SCA Act Overview

As previously mentioned, the SCA was promulgated in 1986 and sought to regulate

---

[98] Robert Gellman, World Privacy Forum, *Privacy in the Cloud: Risks to Privacy and Confidentiality from Cloud Computing* 4 (2009).

[99] *Supra* n. 5.

[100] *Katz v. United States*, 389 U.S. 347 (1967) (applying the Fourth Amendment to telephone conversations); *Smith v. Maryland*, 442 U.S. 735 (1979) (reaffirming and clarifying *Katz*'s holding that the contents of private communications are protected under the Fourth Amendment); *United States v. Jones*, 565 U.S. _(2012) (applying the Fourth Amendment to GPS tracking devices on cars). For a comprehensive legal argument analogizing that under Supreme Court precedent applying the Fourth Amendment to telephone conversations and private conversations, email users possess a reasonable expectation of privacy in the contents of emails stored with an email service provider, *see, Brief of Amici Curiae* Electronic Frontier Foundation, et. al., *In re Application of the United States of America for an Order Pursuant to 18 U.S.C. §2703(d)*, (U.S. District Court for District of CO) (Misc. No. 09-Y-080 CBS) (Apr. 13, 2010).

two uses of computer networks: (1) electronic communication services (ECS) (email and data transmissions), and (2) remote computing services (RCS) (data storage and computer processing).[101] Notably, when the Act was adopted, outsourced computing services were marketed to "businesses of all sizes – hospitals, banks and many others," rather than individuals.[102] Not until 1990, did Internet services become available to consumers.[103] The first step in an analysis is to classify the data into the respective category.[104] It is important to note that web-based email such as Yahoo! and Gmail falls under the category of cloud computing and, therefore, RCS, as addressed in *United States v. Bach*, 310 F.3d 1063 (8th Cir. 2002).[105]

To ensure data privacy, Congress chose to include the RCS category.[106] In order to qualify, four standards must be met: (1) electronic communication systems must be offered publically by the provider as "computer storage or processing services;"[107] (2) data must be received electronically;[108] (3) content is required to be "carried or maintained" by the service provider "solely for the purpose of providing storage or computer processing services" to the client;[109] and (4) the provider cannot be "authorized to access the [client's] content for purposes of providing any services other than storage or computer

---

[101] *Supra* n. 5.
[102] S. Rep. No. 99-541, at 10.
[103] Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 Geo. Wash. L. Rev. 1557, 1572 (2004).
[104] *Id.*, Robison at 1205 (directing to Parts III-IV *infra* for the application of the Act's ECS and RCS categories to cloud computing services).
[105] *United States v. Bach*, 310 F.3d 1063 (8th Cir. 2002) (giving courts initial exposure to the cloud computing environment by examining Fourth Amendment issues addressing Yahoo! Email account webmail seizure).
[106] *See* 18 U.S.C. §§ 2702(a)(2), 2703(b) (2006).
[107] *Id.* §§ 2510(14), 2711(2).
[108] *Id.* §§ 2702(a)(2)(A), 2703(b)(2)(A).
[109] *Id.* §§ 2702(a)(2)(B), 2703(b)(2)(B).

processing."[110] These components lay the foundation for the commercial relationship between the provider and the client. When compared to BAAs in the context of PHI in relation HIPAA and the HITECH Act, the language is likewise narrowly tailored.

Judicial Precedent

Privacy is a fundamental right enumerated in the Fourth Amendment of the United States Constitution. Interpreting this right, the U.S. Supreme Court held in *Katz* that the Fourth Amendment applied to telephone conversations, and later in *Smith*, reaffirming and clarifying *Katz*'s holding that the contents of private communications are protected under the Fourth Amendment.[111]

In general, the crucial element is content versus personal identifying information such as a name, phone number or email address. Under HIPAA and the HITECH Act, Congress has expressed a heightened awareness for protecting PHI.[112] What RCS providers may provide under usual circumstances, does not apply to PHI data. Names and addresses do qualify as PHI. Therefore, an RCS provider cannot voluntarily disclose the user's personal indentifying information to a non-governmental user.

The assertion of non-disclosure of PHI more closely aligns with courts finding "important expectations of privacy in email outside of the Fourth Amendment context."[113] For instance, attorney-client email messages have both subjective and objective expectations of privacy. Several courts have upheld this notion. "Under all of the circumstances, we find that Stentgart could reasonably expect that e-mails she exchanged

---

[110] *Id.*
[111] *Supra* n. 47.
[112] *Supra* n. 1.
[113] *Brief of Amici Curiae* Electronic Frontier Foundation, et. al., *In re Application of the United States of America for an Order Pursuant to 18 U.S.C. §2703(d)*, (U.S. District Court for District of CO) (Misc. No. 09-Y-080 CBS), p. 17-18 (Apr. 13, 2010).

with her attorney on her personal, password-protected, web-based e-mail account, accessed on a company laptop, would remain private."[114] The Southern District of New York echoed the sentiment and held, "in the attorney-client privilege context, that a user "had a reasonable subjective and objective belief that his [Hotmail] communications would be kept confidential."[115] Likewise, email messages containing PHI have a reasonable expectation of privacy.

Terms of Service Agreements and Company Statements

The decreasing role of the personal computer is being replaced by the functionality of the Internet, with web-based email and cloud computing leading the way.[116] "Cloud Computing Services are an emerging network architecture by which data and applications reside on the third party servers, managed by private firms, that provide remote access through web-based devices."[117] The SCA "requires that "storage or computer processing" be the sole reason that a customer transmits her data to the cloud provider."[118] Therefore, it is vital to read both the implied and express consent being given when signing a provider's terms of service, privacy policy and other agreements (i.e., master agreement).[119]

---

[114] *Stentgart v. Loving Care Agency, Inc.*, A-16-09, 2010 N.J. LEXIS 241, *38-39 (N.J. Mar. 30, 2010).
[115] *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F. Supp. 2d 548, 565 (S.D.N.Y. 2008).
[116] Michael Miller, *Cloud Computing: Web-based Applications that Change the Way You Work and Collaborate Online*, p. 11 (2009).
[117] FTC Complaint of Electronic Privacy Information Center at 4, *In re Google, Inc. & Cloud Computing Servs.* (Mar. 17, 2009); *Rearden LLC v. Rearden Commerce*, 597 F. Supp. 2d 1006 (N.D. Cal. 2009) (relaying that cloud computing is "a term used to describe a software-as-a-service (SAAS) platform for the online delivery of products and services."); and *see* Paul Ceruzzi, *A History of Modern Computing*, 318-319; *see e.g.*, 310 F.3d at 1063.
[118] Robison *supra* n. 5.
[119] *Id.* at 1213 (citing, *fn. 129, United States v. Drew*, 259 F.R.D. 449, 462 & n. 22 (C.D. Cal. 2009) (surveying cases in which courts enforced website agreements); *Register.com, Inc. v. Verio, Inc.*, 126 F. Sup. 2d 238, 248 (S.D.N.Y. 2000) (holding that a website user assented to the terms of service by using the provider's service). *But see* Jason Isaac Miller, Note, *Don't Be Evil: Gmail's Relevant Text Advertisements Violate Google's Own Motto and Your E-mail Privacy Rights*, 33 Hofstra L. Rev. 1607, 1632-35 (2005) (arguing that website visitors should not be bound to the Terms of Use agreements for Google's Gmail service because it "provides a flawed registration process that robs prospective users of the opportunity to give informed consent and manifest their agreement.").

These types of agreements can be "classified into three categories: (1) explicit authority to access a customer's data for marketing purposes; (2) vague authority to potentially access a customer's data for marketing purposes; and (3) explicit prohibitions against accessing a customer's data for any purpose other than providing a specific service."[120] Category 1 is the least protective and Google routinely uses these agreements. Their master terms of service ("ToS") agreement stipulates, "Google reserves the right ...to prescreen, review, flag, filter, modify, refuse or remove any or all Content from any [Google] Service."[121] Likewise, Google's Privacy Center alerts customers that Gmail filtering system scans emails to further advertising efforts.[122] This can be problematic for entities who transmit PHI through these avenues, without taking the required measures to encrypt data.

Category 2, while tighter than Category 1, creates a vague middle ground. These providers' agreements reserve the right to access a client's data, but offer no insights as to how or when the authority might be used.[123] Amazon, YouTube and Yahoo! all have policies that fall into this realm.[124]

Finally, Category 3 providers such as Remember the Milk and Mozy, expressly indicate that "We will not view the files that you backup using the Service."[125] Therefore, as Category 1 and Category 3 illustrate, the SCA's protections will likely apply to Category 3

---

[120] *Id.* at 1215.
[121] *Id.* (citing Google Privacy Center: Advertising and Privacy, http://www.google.com/privacy_ads.html and Google Terms of Service).
[122] *Id.*
[123] *Id.* at 1217.
[124] *Id.*
[125] *Id.* (citing Remember the Milk Terms of Use §5, http:///www.rememberthemilk.com/help/terms.rtm; Mozy: Decho Corporation Privacy Policy (Nov. 17, 2008), http://mozy.com/privacy; Zoho Terms of Service (Sept. 7, 2009), http://www.zoho.com/terms.html ("We respect your right to ownership of content created or stored by you. You own the content created or stored by you. Unless specifically permitted by you, your use of the Services does not grant Zoho the license to use, reproduce, adapt, modify, publish or distribute the content created by you or stored in your Account for Zoho's commercial, marketing or any similar purpose.").

where access by the provider is confined to "the underlying storage or computer processing services."[126] Likewise, there is a stronger argument for HIPAA and HITECH compliance, provided other agreements do not contradict the ToS.

Just like service providers must meet strict requirements to qualify as an RCS and enjoy privacy protections for its customers data,[127] so must enterprises engaging in PHI transmission and storage encrypt email and cloud computing storage applications to avoid more severe penalties under the Breach Notification Rule. Moreover, HIPAA business associates and subcontractors are required to comply with 45 C.F.R. §164.504(e), which indicates the privacy terms required in HIPPA business associate agreements, pursuant to Section 13404 of the HITECH Act. Privacy considerations clearly exist for the general public under the Fourth Amendment and the SCA. Even though courts have bound cloud provider clients to the terms of their agreements, if no BAA exists, if a misrepresentation was made about HIPAA and the HITECH Act compliance, or if proper levels of security and privacy were not obtained, then the cloud computing provider is potentially liable. BCE and Salesforce did not execute a BAA, a risk assessment was not conducted and there were no assurances in the contract executed between BCE and Salesforce that all of the requirements of HIPAA and the HITECH Act were satisfied. (Ex.)

Given the personal and sensitive nature of the information being transmitted, the precedents set forth in *Katz* and *Smith*, and the analogous nature of PHI to attorney-client information, all entities either transmitting, receiving, reviewing or storing PHI should be vigilant when conducting HIPAA's required risk analysis.

---

[126] *Id.* at 1220.
[127] *Supra* n. 6.

THE CONSEQUENCES OF THE DEFENDANTS' VIOLATIONS OF HIPAA AND THE HITECH ACT

Ms. Roe's good faith concerns that BCE was in violation of or would violate HIPAA and the HITECH Act and that it had made or would make material, fraudulent representations to customers.

HIPAA

Originally passed in 1996, HIPAA was designed to hold covered entities and their business associates responsible for breaches of PHI. A fundamental purpose of HIPAA is to define and confine the circumstances where PHI may be used or disclosed by covered entities. (45 C.F.R. §164.502(a)). Per the HIPAA Administrative Simplification regulations (45 C.F.R. parts 160, 162 and 164) (HIPAA Rules) at §160.103, a covered entity is a health care provider that "transmits any health information electronically in connection with a covered transaction, such as submitting health care claims to a health plan."

BCE's clients are hospitals and considered covered entities. BCE falls under the HIPAA Rules' definition of a business associate, as "a person who performs functions or activities on behalf of, or certain services for, a covered entity that involved the use or disclosure of individually identifiable health information." (HHS-OCR Privacy Brief, *Summary of the HIPAA Privacy Rule,* p. 3 (2003)). Therefore, the client hospitals (covered entities) and BCE (business associate)

come under the purview of HIPAA.

Individually identifiable health information is information that relates to a medical condition, provision of health care or payment for the provision of care that identifies the individual or there is a reasonable basis to believe can be used for individual identification. (45 C.F.R. §160.103).

The CliniNotes™ program uses PHI as part of its ©Clinical Note because the patient name, date of the note, attending physician and relevant condition are all included. (Ex.) The information is then sent from the hospital to a BCE agent. (Ex.) This information, is then uploaded onto BCE's Salesforce platform, utilized to compile client reports and relied upon when generating statistics such as the number of ©Clinical Notes left on patient charts and the financial impact to the hospital. Therefore, BCE's services, as BCE indicates in its contracts, are required to comply with HIPAA standards. (Ex.)

HIPAA Business Associate Provisions Pre-HITECH Act

Prior to the passage of the HITECH Act, there were two regulations issued by the Secretary of The Department of Health and Human Services (HHS) that impacted the conduct of business associates. The "Privacy Rule" was issued on August 14, 2002 to protect individually identifiable health information. (45 C.F.R. Section 164 Subpart B). And, the "Security Rule," issued on February 20, 2003, established national standards to protect PHI. (45 C. F. R. Section 164 Subpart C). The regulations contained within both the "Privacy Rule" and the "Security Rule,"

applied indirectly to a business associate's conduct. Since the HITECH Act changed the requirements to apply directly to business associates and their subcontractors, these issues are addressed in the HITECH Act section of this Complaint.

The Hospital and Healthsystem Patient Victims of the Defendant's Illegal Conduct Relating to HIPAA and the HITECH Act

While HIPAA has long required the safeguarding of protected health information ("PHI"), Congress saw a need to further augment its rules and regulations to provide even protection for PHI and did so in HITECH, which was enacted in February 2009 to require very stringent data security measures, among other things. One of the HITECH Act's most significant changes to HIPAA's rules and regulations concerns the regulation of *business associates.* A "business associate" is an entity or individual that contracts directly with a covered entity (i.e., a hospital).

Because BCE contracts with HIPAA-covered entities, it is regulated as a "business associate." Similarly, BCE's subcontractors (its physician-educators, Salesforce, Inc., and other independent contractors) are subject to these stringent privacy and security requirements related to PHI. Notably, as of February 17, 2010, HIPAA's "Privacy Rule" and "Security Rule" regulations, and the related civil and criminal penalties for violating these laws, also significantly expanded and were made directly applicable to business associates and their subcontractors. (Section 1301(c) HITECH Act). Another significant new requirement imposed on covered entities and business associates by the HITECH Act is the "Breach Notification Rule" (74 Fed. Reg. 42740, 42760 (Aug. 24, 2009)). Among the new obligations

imposed on business associates and their subcontractors are to provide notice to covered entities, develop and conduct ongoing risk assessments, and individual notification.

To become better acquainted with the current regulations, and begin establishing relationships with hospital in-house counsel, Ms. Roe requested to attend the American Health Lawyers Association meeting in February 2011. (Ex). She learned from leading practitioners at this meeting that BCE needed to address not only the implementation of various initiatives associated with the Affordable Care Act, but also the requirements set out in three areas of law that directly impacted BCE's business: HIPAA/the HITECH Act, cloud computing and electronic data, and social media/electronic discovery. Ms. Roe prepared a memorandum entitled *Potential Legal Issues and Recommendations* explaining this to BCE's partners.

The memorandum initially was submitted to Dr. Weinman on February *27,* 2011 (Ex.) It was revised after a March 16, 2011 conversation with Brad Gross relating to both his and BCE's relationship with Salesforce, Inc. (Exh). Ms. Roe was surprised to discover that while these requirements had been in effect for nearly 18 months, and despite the fact that BCE was marketed to hospitals as a company that provides services to help them meet their healthcare compliance needs, BCE was in violation of many of the HITECH Act's requirements:

- BCE did not have any of these items defined in a protocol included in its quarterly reports to clients,
- BCE didn't discuss or document these items during on-site visits with

clients;

- As of December 5, 2011, BCE still did not meet these significant, mandatory requirements.[128] (Ex.)

BCE's Outside Counsel Letters used for Marketing

BCE had paid Epstein Becker & Green to provide letters about its CliniNotes™ program. In a December 11, 2003 letter, the law firm addressed BCE's clinical documentation improvement program in relation to the risk areas identified by the U.S. Department of Health & Human Services Office of Inspector General's "Compliance Program Guidance for Third-Party Medical Billing Companies." (Ex.) Another letter was issued in January 10, 2011 to supplement this letter. It addressed the use of queries in relation to the "Guidance for Clinical Documentation Improvement Programs" issued by the American Health Information Management Association. (Ex.).

Significantly, in neither letter was the outside law firm asked to (nor did it) address BCE's compliance with HIPAA, HITECH, or the safeguarding of PHI. (Ex.) All communications with Epstein Becker & Green were conducted by BCE's partners and its work was limited in scope, as BCE's General Counsel explained to Ms. Roe on January 9, 2011:

[128] On Wednesday, March 30, 2011, Ms. Roe accompanied Dr. Weinman to a semi-annual visit at Midland Memorial Hospital in Midland, TX. She was present for all meetings with various hospital executives, internal physician coaches, BCE report reviews and other hospital personnel and departments. At no time was there a discussion of a risk assessment in relation to PHI, nor was any inference made about these issues in any of the reports disseminated on the mandatory applicable HITECH requirements. Michael Routh (the Recovery Audit Contractor ("RAC") coordinator for Midland Memorial Hospital) and Ms. Roe discussed RAC compliance and she provided him with a white paper on the subject that she had authored for BCE.

> These are not formal legal opinions, and should not be referred to as such, because a formal legal opinion carries a very different weight than a letter reviewing a process or discussing a subject. . . . There are times when a formal legal opinion is required, but because we were using this primarily for marketing, we did not feel it would be worth spending *$50,000* for a formal opinion (the letter cost us approximately $15,000). (Ex.).

Not only was Ms. Roe concerned about BCE's compliance with HIPAA and HITECH, but, as she discovered, so were some of its customers. In particular, on October 8, 2010, a representative of Tomball Regional Hospital wrote a letter indicating that, "[a]s of today, we have yet to receive documentation satisfying our compliance concerns regarding CliniNotes." (Ex.) In response, Dr. Weinman provided Tomball Regional Hospital's executives with Epstein Becker & Green's January 10, 2011 letter (even though, as noted, the law firm had expressly stated its limitations in the letter: "Please be advised that this letter is directed only to you and your company, and that no third party is entitled to rely on the advice provided herein.") (Ex.). As Mr. Davidson indicated, it was agreed upon that this letter would be used "primarily for marketing" and was subsequently sent to other prospective clients.

On March 4, 2011, in an email sent to Dr. Weinman, Ms. Roe reiterated her concerns about BCE's failure to meet various of the necessary HIPAA/HITECH compliance standards.[129] (Ex.). He asked her to revisit these items at the BCE's

[129] Ms. Roe's concerns about BCE's lack of legal and regulatory compliance were similar to those of Tomball Regional and she was not the only individual to notice such issues. For instance, Mr. Lance H. Roe, a retired hospital CEO with years of service on various boards, attended BCE's March 2011 meeting and presented on items for BCE to consider, which ranged from interacting with executives, to the contract approval process for a capital sale, to obstacles BCE may encounter in the marketplace. Two glaring items that he addressed was BCE's lack of a CEO/corporate structure and its lack of a financial good standing document. Mr. Roe had several individual conversations with BCE's partners, physician educators, and other independent

upcoming partners' meeting on March 17, 2011. (Ex.) In Ms. Roe's memorandum, she made several key recommendations:

- BCE needed to develop and complete Business Associate Agreements with independent contractors, vendors, and clients as mandated by HIPAA;
- BCE needed to conduct background checks for its independent contractors and employees as required by HIPAA/HITECH. *As* she explained, "[b]ecause the data is considered protected health information (PHI), BCE Technology, Inc. is subject to the Department of Health and Human Service Office for Civil Rights implementation of the HITECH Act. Therefore, BCE Technology, Inc. needs to ensure that its products, programs, and representatives comply with HIPAA, HITECH and other relevant regulatory provisions."
- BCE needed to encrypt its email and cloud computing applications;
- BCE needed to provide on-line annual, company-wide HIPAA training because the number of individuals who access or can access PHI and the nature of the information BCE received from its client hospitals;
- BCE needed to obtain a HIPAA compliance certificate for its new website (this was included in the RFP)
- BCE should consider obtaining an Opinion Letter indicating that the CliniNotes Program was compliant with HIPAA and HITECH;

---

contractors about BCE, its structure, long term plans for BCE, Brad Gross's conflict of interest and barriers to entry in new client cultivation. During the course of Ms. Roe's presentation, Mr. Bill Gross turned to Mr. Roe and intimated that he would like to see BCE be acquired by 3M.

- BCE needed to require entities it contracted with to provide proof of their HIPAA compliance;
- BCE needed to use PreCheck to conduct annual background checks; and
- BCE should not adopt a social networking forum on Facebook or Twitter beyond a "place page."

Ms. Roe also cited relevant cases associated with electronic discovery and spoliation of evidence issues.[130] (Ex.). Nevertheless, during her time at BCE she never saw, nor was she made aware of, any BCE document that set out a policy or procedure to address document destruction.

At bottom, and despite Ms. Roe's efforts, only a few of her recommendations were adopted: PreCheck was engaged to perform background checks; and Ms. Roe and Mr. Davidson constructed a *BAA,* which was sent to independent contractors. On the other hand, most of the recommendations were ignored:

- Even though BCE's website designer ("Websults") performed an extensive analysis on BCE's lack of HIPAA compliance and the cost to come into compliance, its suggestions were never fully adopted. (Ex.);
- BCE didn't seek to obtain a HIPAA/HITECH ACT specific opinion letter

[130] *Victor Stanley v. Creative Pipe* (D. Md. Jan. 24, 2011) (awarding over $1 million in attorneys' fees and costs for spoliation for willful loss or destruction); *Rattray v. Woodbury County* (N.D. Iowa, Dec. 27, 2010) (failing to preserve data led to sanctions); and *Rimkus Consulting Group v. Cammarata* (S.D. Tex. Feb. 19, 2010) (discussing Fed. R. Civ. P. 37(e)'s preclusion of sanctions if the loss arises from routine, good faith operation of the computer system and finding the policy of deleting every two weeks after duty aRoe authorized the jury to decide whether to draw an adverse inference).

from its outside counsel (Epstein Becker & Green);

- Encrypted email and privacy disclaimers were not adopted;
- HIPAA training never occurred; and
- HIPAA and PHI document destruction policies were never drafted or added to the draft BCE Operations Manual that Ms. Roe developed and provided to its partners for review. (Ex.) That manual was never approved or distributed.

Instead of engaging in further discussions and establishing procedures about the other areas of HITECH and HIPAA that required compliance, Ms. Roe was instructed by Dr. Weinman to "let it go and focus on generating clients for BCE."

Ms. Roe Worked to Make BCE's Licensing Agreements HIPAA and HITECH Compliant, but BCE's CEO Didn't Want to Use Them

Section 14 of BCE's License and Confidentiality Agreement addresses PHI. As of November 30, 2010, it only addressed HIPAA and was not compliant with the HITECH Act's requirements.[131] Concerned about this fundamental issue, Ms.

ENDNOTES

[131] **HIPAA COMPLIANCE**

a. To the extent required by the provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) 42 U.S.C. 1171 and regulations promulgated thereunder, BCE does hereby assure Hospital that it will appropriately safeguard protected health information, including electronic protected health information ("PHI") made available to or obtained by BCE. Without limiting the obligations of BCE otherwise set forth in this Agreement or imposed by applicable law, BCE agrees to comply with applicable requirements of law relating to BCE and with respect to any task or other activity BCE performs on behalf of Hospital; specifically BCE shall: (i) not use or further disclose PHI other than as permitted or required by this Agreement or as required by law; (ii) use appropriate safeguards to prevent use or disclosure of PHI other than as provided for by this Agreement, and in accordance with the Security Rule set forth at 45 C.F.R Part 160 and 164, Subparts A and C, implement such administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of electronic PHI that it creates, receives, maintains, or transmits on behalf of Hospital; (iii) report to Hospital

Roe met with Mr. Davidson at the March 2011 meeting and they revised BCE's License and Confidentiality Agreement to address the problem.[132]

---

any use or disclosure of PHI not provided for by this Agreement of which BCE becomes aware; (iv) ensure that any subcontractors or agents to whom BCE provides PHI received from Hospital agree to the same restrictions and conditions that apply to BCE with respect to PHI and the safeguarding of electronic PHI; (v) make available PHI in accordance with applicable law; (vi) make BCE's internal practices, books, and records relating to the use and disclosure of PHI received from Hospital available to the Secretary of the United States Health & Human Services for purposes of determining Hospital's compliance with applicable law (in all events, BCE shall immediately notify Hospital upon receipt by BCE of any such request, and shall provide Hospital with copies of any such materials); (vii) incorporate any amendments or corrections to PHI when notified pursuant to applicable law; (viii) make available the information required to provide an accounting of disclosures pursuant to applicable law; and (ix) upon the termination of this Agreement, return or destroy all PHI received from Hospital that BCE still maintains in any form and retain no copies of PHI.

b. Without limiting the rights and remedies of Hospital set forth elsewhere in this Agreement or available under applicable law, Hospital may terminate this Agreement without penalty or recourse to Hospital if Hospital determines that BCE has violated a material term of the provisions of this Section 13 of this Agreement BCE agrees that this Agreement may be amended from time to time by Hospital if and to the extent required by the provisions of HIPAA and the regulations promulgated thereunder, in order to assure that this Agreement is consistent therewith.

c. While performing its duties and obligations under this Agreement, BCE shall, and shall cause its employees, agents, and subcontractors to, comply with all laws and regulations that apply to the confidentiality and security of patient information, including HIPAA, which are now in force or which may subsequently be in force. The parties agree that if necessary, they shall amend this Agreement to comply with or effectuate HIPAA and the regulations issued under it.

[132] **HIPAA and HITECH ACT COMPLIANCE**

a. To the extent required by the provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) 42 U.S.C. 1171 The American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 111th Cong., 1st Sess. (Feb. 19, 2009) [hereinafter, ARRA] (including the HITECH Act), and regulations promulgated thereunder, BCE does hereby assure Hospital that it will appropriately safeguard protected health information, including electronic protected health information ("PHI") made available to or obtained by BCE. Without limiting the obligations of BCE otherwise set forth in this Agreement or imposed by applicable law, BCE agrees to comply with applicable requirements of law relating to BCE and with respect to any task or other activity BCE performs on behalf of Hospital; specifically BCE shall: (i) not use or further disclose PHI other than as permitted or required by this Agreement or as required by law; (ii) use appropriate safeguards to prevent use or disclosure of PHI other than as provided for by this Agreement, and in accordance with the Security Rule set forth at 45 C.F.R. Part 160 and 164, Subparts *A* and C, implement such administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of electronic PHI that it creates, receives, maintains, or transmi ts on behalf of Hospital; (iii) report to Hospital any use or

Ms. Roe also raised legal concerns about BCE's standard business contract language with Dr. Weinman on numerous occasions. On April 18, 2011, after BCE's client contract language, Dr. Weinman instructed her to use "an edited version I sent this am" and added that he would "take responsibility." (Ex.) The same thing happened with BCE's NMMC contract and its LifePoint contract. (Ex.) Significantly, the language that Dr. Weinman removed related to disclosing BCE's relationship with Salesforce, Inc. and using their platform for the CliniNotes2.0 application. Disclosure of sub-contractors, especially those hosting PHI, is required in the HITECH Act.

As demonstrated in BCE's *The CliniNotes™ Documentation Process,* once a

---

disclosure of PHI not provided for by this Agreement of which BCE becomes aware; (iv) ensure that any subcontractors or agents to whom BCE provides PHI received from Hospital agree to the same restrictions and conditions that apply to BCE with respect to PHI and the safeguarding of electronic PHI; (v) make available PHI in accordance with applicable law; (vi) make BCE's internal practices, books, and records relating to the use and disclosure of PHI received from Hospital available to the Secretary of the United States Health & Human Services for purposes of determining Hospital's compliance with applicable law (in all events, BCE shall immediately notify Hospital upon receipt by BCE of any such request, and shall provide Hospital with copies of any such materials); (vii) incorporate any amendments or corrections to PHI when notified pursuant to applicable law; (viii) make available the information required to provide an accounting of disclosures pursuant to applicable law; and (ix) upon the termination of this Agreement, return or destroy all PHI received from Hospital that BCE still maintains in any form and retain no copies of PHI.

b. Without limiting the rights and remedies of Hospital set forth elsewhere in this Agreement or available under applicable law, Hospital may terminate this Agreement without penalty or recourse to Hospital if Hospital determines that BCE has violated a material term of the provisions of this Section 13 of this Agreement. BCE agrees that this Agreement may be amended from time to ti me by Hospital if and to the extent required by the provisions of HIPAA and the regulations promulgated thereunder, in order to assure that this Agreement is consistent therewith.

c. While performing its duties and obligations under this Agreement, BCE shall, and shall cause its employees, agents, and subcontractors to, comply with all laws and regulations that apply to the confidentiality and security of patient information, including HIPAA, which are now in force or which may subsequently be in force. The parties agree that if necessary, they shall amend this Agreement to comply with or effectuate HIPAA and the regulations issued under it.

client's Health Information Management Department reviews patient charts for accuracy in how required coding entries are made for various procedures and co-ordinates with the physician coach, the Clinical Notes© are sent to BCE for review. (Ex.)

BCE's Procedures for the Transmission / Review of Client's PHI Violate HIPAA

BCE's procedures for how it dealt with clients' PHI differed only in form, not substance after January 21, 2011. They failed to comply with HITECH's and HIPAA's security and privacy mandates since BCE didn't encrypt its emails, had not performed an internal or external risk assessment for PHI vulnerability, and failed to disseminate or make a privacy/confidentiality statement. Client PHI sent before January 21, 2011 was in the form of BCE's CliniNotes™ and received into personal, unsecure email accounts (such as "att.net", "gmail.com" and "bcetechnology.com"). (Ex.)

Brad Gross is BCE's Account Administrator for the"bcehealthcareadvisors.com" email, which used Gmail, a free service offered by Google. (Ex.)On January 21, 2011, he sent an email indicating that he was "migrating all of us onto a new setup which will allow a number of new features: a well-developed and strong spam filter, global calendar, strong integration with Microsoft Outlook and good integration with Blackberry." (Ex.) Mr. Gross made no mention of encryption, privacy or confidentiality disclaimers. He also provided *BCE's Email Manual,* which also failed to address these items. (Ex.)

BCE Put Its Clients at Risk of Regulatory Action and Litigation

To illustrate the potential magnitude of the risks that BCE exposed its clients to by continuing to violate HIPAA and HITECH Act's requirements, information provided by BCE's Director of Technology reflects that in 2009 BCE reviewed 48,000 medical records provided by clients and made 28,000 clinical improvement suggestions, which led to a confirmed increase of $91,000,000 in increased Diagnosis Related Group ("DRG") net revenue for its client hospitals. (Ex.)

This means that over a six year period, approximately 180,000 Clinical Notes© containing PHI (i.e., information about the date, patient's identity, his or her treating physician and the patient's relevant condition) were reviewed by BCE during this period to provide clinical feedback or enter the information into coaching logs for client-reporting purposes.[133] BCE's client hospitals, such as Beaufort, sent such notes to BCE every 1-2 weeks. (Ex.) Another BCE client hospital, St. Vincent's, sent the PHI via email. (Ex.)

It is again worth noting that BCE lacked HITECH's mandatory administrative, physical and technical safeguards for how to safeguard the disposal of PHI; moreover, BCE never conducted the mandatory internal or external risk assessment protocol, it lacked a breach notification procedure, and had not developed breach logs.

Ms. Roe did include a section in the proposed operations manual, "Anyone working with patient records must comply with HIPAA standards. In general, this means not disclosing a patient's identity to anyone outside of those involved in the

[133] PHI received was typically viewed by Dr. Weinman, Debra Hartz, and Michelle Strickland at their homes while family members, who are not affiliated business associates or employees, were present.

treatment protocol." (Ex.) Ms. Roe was instructed that anything related to the CliniNotes™ program clinical implementation, delivery and process was handled by Dr. Weinman. The issue of Ms. Roe contributing to any discussions related to clinical items or the CliniNotes™ program was discouraged. (Ex.)

Despite BCE's continued lack of adherence to HIPAA and the HITECH Act, Ms. Roe continued to make BCE's partners and its clients aware of the law surrounding HIPAA concerns and the steep penalties for violating it on BCE's website. On November 5, 2011, for instance, she posted a short piece entitled *Texting – Another Potential Way to Violate HIPAA.* (Ex.) As a follow-up, on November 21, 2011, she posted *HIPAA Alert: increased fines, audits and criminal indictments.* (Ex.), which specifically advised that "educating everyone on the legal and monetary ramifications of breaching HIPAA privacy standards and accessing medical records."

Defendants' Failure to Perform Required and Adequate Risk Assessments, Which Put Covered Entity Patients and Salesforce Shareholders at Risk

A risk assessment should be conducted in a manner similar to doing "[d]ue diligence in the context of mergers, acquisitions, divestitures or joint ventures (strategic initiatives)."[134] Due diligence, when approached from both the strategic initiative buyer's and seller's standpoint, has been defined as the "affirmative duty to ensure compliance with disclosure obligations and the investigation that is part of nearly every … corporate acquisition, whether out of an affirmative duty or a thought to a future defense."[135]

---

[134] American Health Lawyers Association, *Enterprise Risk Management for Healthcare Entities*, p. 385 (1st Ed. 2009).

[135] *Id.* citing, Katz, David A., *Due Diligence In Acquisition Transactions*, Practicing Law Institute PLI Course Handbook, Conducting Due Diligence 2003, p. 579-580 (Jun. 2007).

Likewise, the HITECH Act's Breach Notification Rule requires each contracting party to conduct a risk assessment; hence, providing assurances of compliance with the expanded HIPAA Privacy and Security Rules requirements.

Violating the technical requirements and/or causing or discovering a related incident consistent with breaching the provisions defined in HIPAA and the HITECH Act, exposes covered entities, business associates and subcontractors to increased government enforcement.

"This new federal law [the HITECH Act] holds covered entities and business associates accountable to the Department and to individuals for proper safeguarding of the private information entrusted to their care."[136] A primary objective of HIPAA is to define and confine the circumstances where PHI may be used or disclosed by covered entities, business associates and subcontractors.[137] In determining whether a person is the agent of the covered entity or business associate, the federal common law of agency is used.[138]

A covered entity, according to the HIPAA Administrative Simplification Regulations, is a healthcare provider that "transmits any health information electronically in connection with a covered transaction, such as submitting health care claims to a health plan."[139] Under the HIPAA Rules, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services are

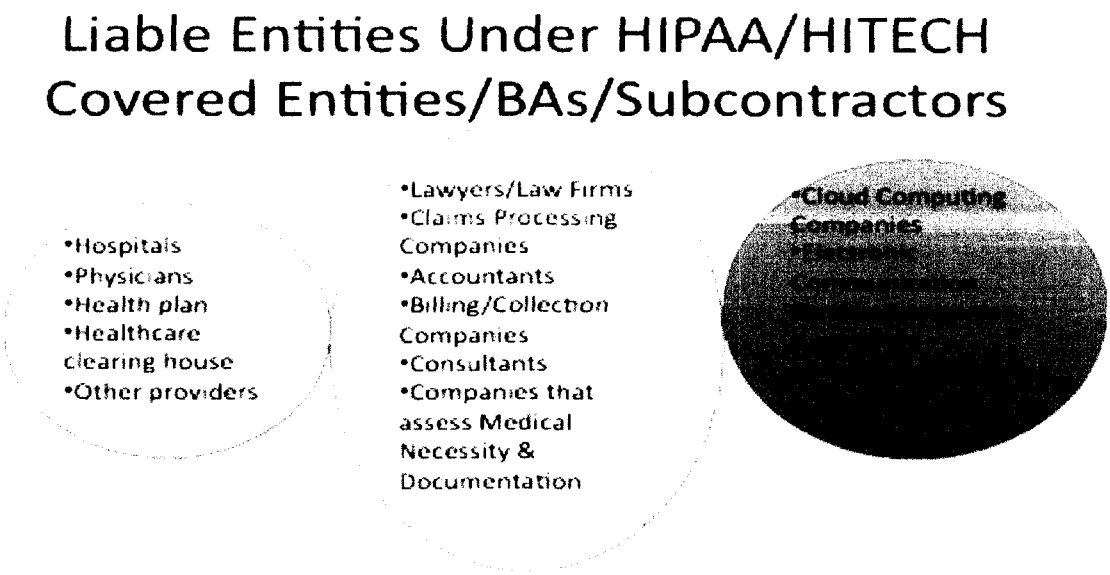
---

[136] David Blumenthal, National Coordinator for Health Information Technology and Georgina Verdugo, Director, Office for Civil Rights, U.S. Department of Health and Human Services, *Building Trust in Health Information Exchange- Statement on Privacy and Security* (Jul. 8, 2010).
[137] 45 CFR §164.502(a).
[138] 45 C.F.R. § 164.404(a)(2).
[139] 45 CFR parts 160, 162 and 164) (HIPAA Rules) at §160.103.

considered business associates. Business associates are defined as "a person who performs functions or activities on behalf of, or certain services for, a covered entity that involved the use or disclosure of individually identifiable health information."[140]

Under the HITECH Act, the "snitch provision" of the HIPAA "Privacy Rule" applies equally to a business associate as it does to a covered entity.[141] Consequently, both the covered entity and the business associate have an affirmative duty to take reasonable steps to cure a breach or other violation. The chart illustrates the three types of entities that fall under the purview of HIPAA and the HITECH Act. Notably, the actions or inactions of one group may adversely affect another group.

[140] HHS-OCR Privacy Brief, *Summary of the HIPAA Privacy Rule*, p. 3 (2003) (explaining that persons or organizations do not qualify as business associates if their functions or services do not involve the use or disclosure of protected health information, and where any access to protected health information by such persons would be incidental, if at all).
[141] HITECH Act 13404(b), citing the HIPAA "Privacy Rule" provision 164.504(e)(1)(ii).



Recent Minnesota Attorney General Filing Against Accretive, Inc. for HIPAA and the HITECH Act Violations

Recent actions by the Minnesota (MN) Attorney General highlight the notion that covered entities are not the only group that needs to comply with the provisions set forth in HIPAA and the HITECH Act.[142] Here, the Attorney General alleged that Accretive Health, Inc. ("Accretive") violated HIPAA and the HITECH Act as a business associate for exposing more than 25,000 patients' PHI from two MN hospitals with whom it had business associate agreements.[143] The crux of the claim focused on Accretive's failure to comply with the regulations in relation to implementing and maintaining appropriate administrative technical and physical safeguards, such as encryption, for PHI after agreeing with two covered entities that "it would not use or disclose protected health

[142] 45 CFR §160.404; *State of Minnesota v. Accretive Health, Inc.*, Complaint, 3, 19-20 (U.S. District Court of MN (Jan. 19, 2012)) (showing that PHI data violations were discovered on "at least 23,531 Fairview and North Memorial patients" and, North Memorial's expert "discovered an additional 6,690 patients whose names and data were believed to be on the laptop but who were not revealed to be on the laptop by Accretive.").
[143] *Id.*

information in violation of HIPAA or HITECH and that *it would use "appropriate safeguards" to prevent the misuse or disclosure of protected health information*" (emphasis added)."[144]

Just as there are fundamental inquires in a due diligence process of a strategic initiative, there are basic questions affiliated with HIPAA and the HITECH Act's reasonable diligence in risk assessments. These include:

- Have you identified the ePHI within your organization? This includes ePHI that you create, receive, maintain or transmit.
- What are the external sources of ePHI? For example, do vendors or consultants create, receive, maintain or transmit ePHI?
- What are the human, natural and environmental threats to information systems that contain ePHI?[145]

It is the responsibility to provide annual guidance on HIPAA Security Rule provisions.[146] In 2010, the Office of Civil Rights (OCR), released guidance on HIPAA's risk analysis requirements, which built upon on the foundation set forth by the National

---

[144] *Id.* at 20.
[145] National Institute of Standards and Technology, *SP 800-30 – Risk Management Guide for Information Technology Systems*, available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidancehtml; Office of Civil Rights, *Guidance on Risk Analysis Requirements under the HIPAA Security Rule* (Jul. 14, 2010).
[146] 45 C.F.R. §§ 164.302-318

Institute of Standards and Technology (NIST). [147] Evaluation of risks and vulnerabilities are required, as are an organization's implementation of reasonable and appropriate security measures subject to the Security Rule.[148] The Security Rule expressly requires entities to, "[c]onduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the [organization]."[149] Meaning, a risk analysis, which meets the OCR, NIST and other regulatory guidelines is required.

Likewise, BCE, its client hospitals and Salesforce.com failed to comply with the provisions set forth in HIPAA and the HITECH Act. Similar to Accretive, the Defendants failed to conduct the required risk assessments, implement the statutory protective and disposal measures of PHI and ePHI and failed to encrypt its electronic transmissions of ePHI.

Fraud in the Inducement

The requirements for maintaining a cause of action for fraud (including fraudulent inducement) in Pennsylvania, include the following elements that the plaintiff must allege: (1) a representation; (2) which is material to the transaction at hand; (3) made falsely, with knowledge of its falsity or recklessness as to whether it is true or false; (4) with the intent of misleading another into relying on it; (5) justifiable reliance on the misrepresentation; and (6) the resulting injury was proximately caused by the reliance. Bortz v. Noon, 556 Pa. 489, 499, 729 A.2d 555, 560 (1999).

---

[147] National Institute of Standards and Technology, *SP 800-30 – Risk Management Guide for Information Technology Systems*, available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidancehtml; Office of Civil Rights, *Guidance on Risk Analysis Requirements under the HIPAA Security Rule* (Jul. 14, 2010).
[148] *Id.*
[149] 45 C.F.R. § 164.308(a)(1)(ii)(A)

BCE's *License and Confidentiality Agreement* made a representation that BCE and its CliniNotes Program complied with HIPAA and the HITECH Act. It is material because the program involves the review of protected health information (PHI) that is sent from the hospital to the CEO or CMO of BCE. It was made falsely because Herb Weinman provided a letter on Jane's behalf to show to clients in December 2010, Jane raised the HIPAA/HITECH Act compliance issues with BCE's partners, which include the general counsel and CEO, and even after the *Agreement* was updated to include the HITECH Act, the items that needed to be addressed in relation to HIPAA/HITECH were never implemented; yet, BCE officers continued to have clients (new and renewal) sign the contract with the knowledge that the provisions were false. The intent of misleading current and new clients to sign a contract to generate revenue is apparent and it is justifiable that clients would rely on the misrepresentation given the significance of HIPAA, the HITECH Act, and PHI. Finally, the clients and subcontractors liability exposure under HIPAA, the HITECH Act would be proximately caused by the reliance on BCE's representations in its *Agreement* and other materials.

Because all six elements are met, there is a strong case that BCE would be liable under PA law for fraudulent inducement.

Ms. Roe Brings up the Misrepresentations of Case Mix Data Provided to Clients

Case mix index (CMI) can be defined as, "[i]ndividual inpatient discharges [that] are associated with a Diagnosis Related Group (DRG) that classifies patients that use similar hospital resources into the same group (*e.g.*, DRG 7 refers to lung transplants). Each

DRG has an associated DRG-weight, which reflects the estimated relative costliness of patients in that DRG compared with the average Medicare patient across the country. CMI provides the average DRG weight for the hospital, calculated as the sum of all DRG weights for Medicare discharges divided by the total number of discharges."

In essence, the DRGs that are submitted to Medicare form the basis of the cost report. DRG codes are based on ICD-9 codes currently (ICD-10 implementation has been delayed). Based upon what language a physician (or, depending on the state, an advanced practitioner such as a nurse practitioner or a physician's assistant) uses in the patient chart/medical record, a particular ICD-9 code is assigned. Physician billing codes are different and are known as CPT codes. Different codes carry different values for payment. Therefore, the language dictates the code and modifiers that are submitted to government and private insurers for payment.

According to an industry expert,

> *The CMI is not on the cost report but all hospitals maintain that stat for Total hospital, Medicare, Medicaid, and other payers. It is a very important stat.*
>
> *If the DRGs are not documented or coded correctly the CMI can over or understated which means that the hospital may be over or under paid.*

CMI is also used by hospitals to gauge utilization and compare performance with other hospitals, relied upon by Recovery Audit Contractors (RACs) and other auditors and is the benchmark that is used by clinical documentation improvement programs. In relation to clinical documentation improvement (CDI) programs, CMI data is used in both marketing and as a bench mark for clients to see changes in reimbursement based

on changes in clinical documentation.

On September 13, 2011, Ms. Roe brought up problems she had discovered about the Medicare Case Mix Data that had been represented to BCE's then-customer, the Scott and White Clinic to the attention of Dr. Weinman. (Ex.) In turn, Or. Weinman addressed the issue with Bill Gross, who responded, "AHD has all MC discharges SW only tracked Med Surg with CliniNotes. No discrepancy I am sure Ms. Roe understands and conveys to clients." (Ex.)

Ms. Roe forwarded his response to one of BCE's independent physician contractors, Mark Smith, MD for a second perspective. Dr. Smith responded,

> "No, I don't understand. *Does this mean we are playing funny business with the numbers?* If we are portraying them as the hospital CMI, it should be the hospital CMI. Why wouldn't they keep up with their whole CMI for the hospital? *This may be one of our credibility problems if hospitals try to compare the numbers and they aren't the same."* (Ex.) (Emphasis added).

After Ms. Roe relayed her concerns about these material misrepresentations concerning Medicare data to Dr. Weinman and Dr. Smith had expressed similar concerns, BCE's partners met during September 16-17, 2011 at its Fall Meeting in Wilkes-Barre, PA. Following this meeting, Ms. Roe was told to perform "cold calls" on potential client hospitals for a six-week period, and she complied. (Ex) She continued to make progress with potential clients she had been cultivating for months, while promoting BCE at various speaking engagements, and receiving positive feedback from individuals both external and internal to BCE. (Ex) These included a hand-written note from a hospital CEO, comments from physician

educators who had co-presented with her on various occasions, and emails from current contacts. (Ex.)

THE CONSEQUENCES OF THE DEFENDANTS' VIOLATIONS OF THE FEDERAL TRADE COMMISSION ACT

The Federal Trade Commission Act gives the Federal Trade Commission ("FTC") "the authority to prohibit unfair or deceptive practices in or affecting commerce." (15 U.S.C. § 45(a)(1)). Unfair or deceptive practices are further delineated to include acts that either actually cause or likely cause reasonable foreseeable injury or involve material conduct. All of BCE's client hospitals, subcontractors, and outside counsel are located within the United States. Payment is rendered by client hospitals to BCE for its CliniNotes™ product and educational services. Services or products are provided by subcontractors in relation to an aspect of the CliniNotes™ program in exchange for compensation. Therefore, the FTC has the authority to consider the acts of BCE, its clients and its subcontractors in relation to its deceptive practices of claiming to be a compliance company that works with PHI; but, in reality, violating both HIPAA and the HITECH Act for several years and causing actual and foreseeable harm to both patient's individually identifiable health information and its clients.

In 2009, the FTC brought a claim against CVS Caremark Corporation for failing to provide reasonable and appropriate security for personal information obtained during the regula r course of business of selling prescription medications. *(In the Matter of CVS Caremark Corporation* (Jun. *18,* 2009). In particular, the FTC focused on the privacy and confidentiality of personal information statement that was disseminated and relied upon by consumers. *Id.*

> CVS/pharmacy wants you to know that nothing is more central to our operations than maintaining the privacy of your health information ("Protected Health Information" or "PHI"). PHI is information about you, including basic information that may identify you and relates to your past, present or future health or condition and the dispensing of pharmaceutical products to you. We take this responsibility very seriously.

The FTC determined that CVS had engaged in a myriad of practices that ran inapposite to its representation about privacy concerns. *Id.* at 2. Specifically, respondent failed to: (1) implement adequate policies and procedures to dispose of PHI; (2) adequately train employees; (3) use reasonable measures to assess compliance; or (4) employ a reasonable process for discovering or remedying risks to such information. Ultimately, it was found that CVS inappropriately discarded PHI as a result of the policy and procedure failures.

BCE, its client hospitals, and its subcontractors, including Salesforce, mirror those of CVS. BCE represents in its *License and Confidentiality Agreement* (standard client contract) that they are compliant with HIPAA and HITECH. BCE did not implement adequate policies and procedures, failed to adequately train employees, did not perform an internal or external risk assessment with client hospitals or subcontractors to measure compliance, and did not employ a reasonable process for discovering or remedying such information. Therefore, BCE, its client hospitals, and its subcontractors, including Salesforce and outside counsel, should be found to have violated the Federal Trade Commission Act for engaging in deceptive trade practices.

BCE PARTNERS' REPEATED BREACHES OF FIDUCIARY DUTIES

AND FAILURE TO UPHOLD CORPORATE RESPONSIBILITIES

BCE's Failure to Adhere to Corporate Formalities and Piercing the Corporate Veil

In Pennsylvania, the seminal case that is continually referenced is *Lumax Industries v. Aultman*, 543 PA. 38, 41-42, 669 A.2d 893, 895 (Pa. 1995). Under Pennsylvania law, the following factors are to be considered in determining whether to pierce the corporate veil: (1) undercapitalization; (2) failure to adhere to corporate formalities; (3) substantial intermingling of corporate and personal affairs; and (4) the use of the corporate form to perpetrate a fraud. *Id.* In order to withstand a demurrer, plaintiff must set forth conduct which Katz allegedly engaged in that would bring his actions within the parameters of a cause of action based on a theory of piercing the corporate veil. While it is not necessary to set forth the evidences to be proved, it is essential that the facts the pleader depends upon to show liability be averred. *Id.* at 893.

While there is a presumption against piercing the corporate veil in PA, the PA Supreme Court has set forth specific parameters and four instances where the corporate veil may be pierced. The second is "failure to adhere to corporate formalities" and it must be supported by the facts. Chuck's emails expressly support that the corporate formalities were not observed. Additionally, during the course of discovery, it is highly probable that "substantial intermingling of personal and corporate affairs" occurred, that it was undercapitalized, and given that they represented themselves as a compliance company, yet did quite the opposite, it is likely these other instances are applicable.

A claim against BCE for piercing the corporate veil can be upheld. These same principles apply to judgments obtained in bankruptcy.

Dr. Weinman Instructs Ms. Roe to "Stop Playing Lawyer"

On Monday, September 19, 2011, Dr. Weinman told Ms. Roe in a phone conversation that, as the messenger for BCE's partners, she should "quit playing lawyer." Nearly one-month after the Medicare fraud was reported, Bill Gross sent out an email with the corrected items and indicated the start and end dates for Scott & White Health Clinic. (Ex.)

When Ms. Roe asked certain questions about how this had happened, she got preposterous answers. (Ex.) All that was required was entering data from a database into the correct years and running an average. But that was not the explanation she received. (Ex.) She was told that this was information to use going forward; not to address it on the October Sales Call; and not to reach out to entities considering the program and provide them with corrected data. Ms. Roe, however, mentioned it on the sales call and felt compelled to send out corrected data to certain entities so that they could ensure that any information being reported to Medicare and other programs was accurate and compliant with their obligations under law. (Ex.)

Records Start being Deleted

Ironically, when a snapshot of the screen was taken from the dates that she sent the information, there was no trail. (Ex.) Ms. Roe had already forwarded the email to her personal account or had sent the data hardcopy through the mail. (Ex.) Later, Dr. Weinman said that he had "accidentally" deleted several emails: On December 4, 2011, he asked for contact information for VHA-Unify, saying that he "accidentally deleted many emails." (Ex.) He later indicated that he had found another item "in the trash!" (Ex.)